

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-237228
 (43)Date of publication of application : 09.09.1997

(51)Int.CI.

G06F 12/14
 G06K 17/00
 G09C 1/00
 G09C 1/00
 H04L 9/08
 H04L 9/32

(21)Application number : 08-042913

(71)Applicant : TOSHIBA CORP

(22)Date of filing : 29.02.1996

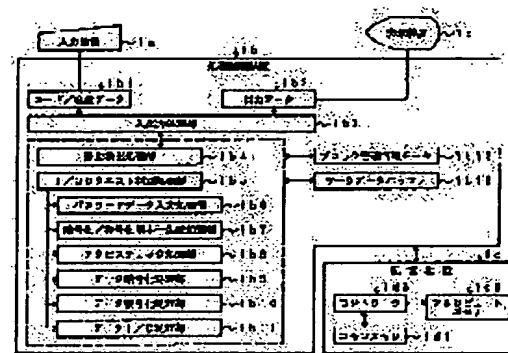
(72)Inventor : MIURA YOSHIYUKI

(54) ACCESS CONTROL METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To improve the security of a portable storage medium such as a PC card.

SOLUTION: At the time of formatting the PC card 1d, a user is allowed to input password data used for generating key data for ciphering/decoding for ciphering and decoding processings. Inputted password data is stored in the PC card 1d, key data for ciphering/decoding is generated by using the data and key data is announced to the user. When the user requests writing to the PC card 1d, it is confirmed whether password data exists in the PC card 1d or not. When it is stored, the user is allowed to input key data for ciphering/decoding and access right to the PC card 1d is checked. When they are matched as a result, data is ciphered by using key data and data is written in the PC card 1d.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平9-237228

(43)公開日 平成9年(1997)9月9日

(51)Int.Cl. ⁶	識別記号	序内整理番号	F I	技術表示箇所
G 06 F 12/14	3 2 0		G 06 F 12/14	3 2 0 B 3 2 0 C
G 06 K 17/00			G 06 K 17/00	E
G 09 C 1/00	6 3 0	7259-5 J	G 09 C 1/00	6 3 0 Z
	6 6 0	7259-5 J		6 6 0 A

審査請求 未請求 請求項の数 3 OL (全 11 頁) 最終頁に続く

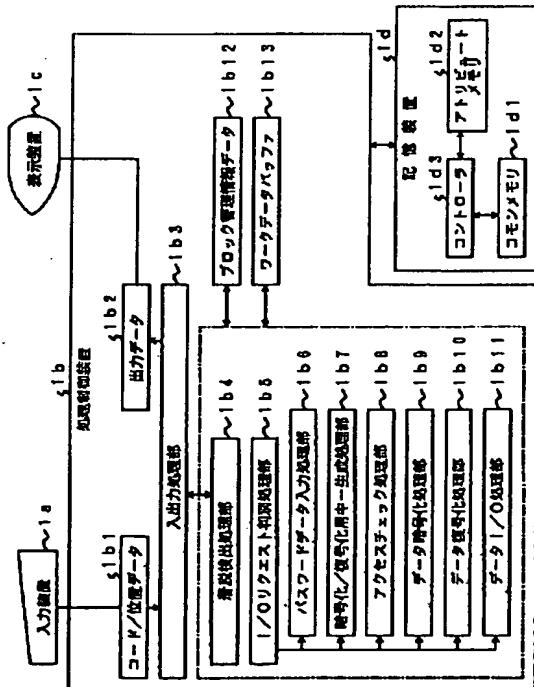
(21)出願番号	特願平8-42913	(71)出願人	000003078 株式会社東芝 神奈川県川崎市幸区堀川町72番地
(22)出願日	平成8年(1996)2月29日	(72)発明者	三浦 佳之 東京都青梅市末広町2丁目9番地 株式会社東芝青梅工場内
		(74)代理人	弁理士 鈴江 武彦

(54)【発明の名称】 アクセス制御方法

(57)【要約】

【課題】 PCカードなどの可搬型記憶媒体に対するセキュリティ性の向上を図る。

【解決手段】 PCカード1dのフォーマット時は、その暗号化および復号化処理のための暗号化／復号化用キーデータを生成に用いるパスワードデータをユーザに入力させる。そして入力されたパスワードデータをPCカード1d内に格納すると共に、そのデータを利用して暗号化／復号化用キーデータを生成し、そのキーデータをユーザにアナウンスする。ユーザがPCカード1dに対してライトリクエストした場合には、PCカード1d内にパスワードデータが存在するかを確認し、格納されている場合にユーザに暗号化／復号化用キーデータを入力させ、PCカード1dへのアクセス権をチェックする。その結果一致していたならば、キーデータを使用してデータを暗号化した後、PCカード1d内にライトする。



【特許請求の範囲】

【請求項 1】 可搬型記憶媒体が取り外し自在に装着される計算機システムで使用されるアクセス制御方法において、

ユーザからの入力パスワードに基づいて前記可搬型記憶媒体に格納するデータを暗号化／復号化するためのキーデータを生成してそれをユーザに提示すると共に、前記入力パスワードを前記可搬型記憶媒体に格納することによって、前記可搬型記憶媒体を初期設定し、

前記初期設定された可搬型記憶媒体が前記計算機システムに装着されたとき、あるいは前記装着された可搬型記憶媒体に対するデータ書き込み／読み出し要求が発行されたとき、前記可搬型記憶媒体から読み出した入力パスワードから暗号化／復号化用キーデータを生成し、その生成した暗号化／復号化用キーデータとユーザから入力される暗号化／復号化用キーデータとの比較結果に基づいて前記可搬型記憶媒体に対するアクセス権の有無を判定し、

アクセス権を有すると判定したとき、前記可搬型記憶媒体に対するデータ書き込み／読み出し要求に応じてライトデータの暗号化およびその暗号化データの書き込み／暗号化データの読み出しおよびその復号化を行うことを特徴とするアクセス制御方法。

【請求項 2】 前記可搬型記憶媒体の着脱を検出し、前記可搬型記憶媒体が装着される度に前記アクセス権有無の判定処理を行うことを特徴とする請求項 1 記載のアクセス制御方法。

【請求項 3】 PCカードが取り外し自在に装着される計算機システムで使用されるアクセス制御方法において、

ユーザからの入力パスワードに基づいて前記PCカードに格納するデータを暗号化／復号化するためのキーデータを生成してそれをユーザに提示すると共に、前記入力パスワードを前記PCカードに格納することによって、前記PCカードを暗号化カードとして初期設定し、

前記初期設定されたPCカードが前記計算機システムに装着されたとき、あるいは前記装着されたPCカードに対するデータ書き込み／読み出し要求が発行されたとき、前記PCカードから読み出した入力パスワードから暗号化／復号化用キーデータを生成し、その生成した暗号化／復号化用キーデータとユーザから入力される暗号化／復号化用キーデータとの比較結果に基づいて前記PCカードに対するアクセス権の有無を判定し、

アクセス権を有すると判定したとき、前記PCカードに対するデータ書き込み／読み出し要求に応じてライトデータの暗号化およびその暗号化データの書き込み／暗号化データの読み出しおよびその復号化を行うことを特徴とするアクセス制御方法。

【発明の詳細な説明】**【0001】**

【発明の属する技術分野】 この発明は、可搬型記憶媒体が取り外し自在に装着される計算機システムで使用されるアクセス制御方法に関する。

【0002】

【従来の技術】 従来、半導体メモリを内蔵したPCカードやフロッピーディスクなどの可搬型記憶媒体に対するデータ書き込みにおいては、書き込みデータを変形させることなく、そのままの状態で記憶媒体に格納するという方式が採用されており、データを書き込んだユーザ以外の他のユーザでも簡単にそのデータに対してアクセスすることができた。なお、この方式におけるデータセキュリティ方式としては、書き込み禁止や隠しファイルなど、それぞれのファイルまたはディレクトリ毎に属性情報を変更することにより、他のユーザからのアクセスを制限するというものが知られている。

【0003】 しかしながら、このようなセキュリティ方式を採用しても、PCカード内やフロッピーディスクのデータ構成は誰でも容易に確認することができ、かつ、それらの属性も容易に変更することができるため、十分な秘匿性を得ることはできなかった。

【0004】 また、セキュリティを考慮したデータの格納方式としては、PCカードなどの記憶媒体内にパスワードデータを格納し、アクセス時にパスワード入力をすることにより、その記憶媒体に格納されているパスワードとの照合を行い、アクセス権をチェックした後、データライトおよびリードを行う方式が知られている。さらに、記憶するファイルまたはディレクトリ毎に暗号化処理を行うことにより他のユーザがアクセスしても有効なデータを取得することができないようにする方式もある。なお、この時に使用される暗号化用のキー（鍵）データは、それぞれファイルまたはディレクトリの属性情報として付加され、これを取得することにより、暗号化後のデータの復号化が実現される。

【0005】 しかし、これらのセキュリティ方式においては、PCカードなどの記憶媒体内にパスワードまたは暗号化／復号化用キーデータ自体を格納しているため、I/Oアクセス時には解析できないものの、記憶媒体内のデータを解析することにより、それらの取得を行うことができ、その後容易にデータをアクセスすることができる。つまり、単一レベルでの秘匿しか行っていなかっため、容易にそれを解除することができ、これも秘匿性の低いものであった。

【0006】

【発明が解決しようとする課題】 上述したように、半導体メモリを内蔵したPCカードやフロッピーディスクなどの可搬型記憶媒体に対する従来のセキュリティ方式では、第三者が容易に属性を変更することができますたり、パスワードや暗号化用のデータを解析し取得することができるため、個人単位で携帯する可搬型記憶媒体の個人情報を秘匿化するセキュリティ技術としては信頼性の低い

ものであった。

【0007】この発明はこの様な点に鑑みてなされたものであり、個人単位で携帯され、且つ計算機システムに着脱自在に装着して使用されるという特徴を持つ可搬型記憶媒体のセキュリティー保持に適したアクセス制御方法を提供することを目的とする。

【0008】

【課題を解決するための手段】この発明は、可搬型記憶媒体が取り外し自在に装着される計算機システムで使用されるアクセス制御方法において、ユーザからの入力パスワードに基づいて前記可搬型記憶媒体に格納するデータを暗号化／復号化するためのキーデータを生成してそれをユーザに提示すると共に、前記入力パスワードを前記可搬型記憶媒体に格納することによって、前記可搬型記憶媒体を初期設定し、前記初期設定された可搬型記憶媒体が前記計算機システムに装着されたとき、あるいは前記装着された可搬型記憶媒体に対するデータ書き込み／読み出し要求が発行されたとき、前記可搬型記憶媒体から読み出した入力パスワードから暗号化／復号化用キーデータを生成し、その生成した暗号化／復号化用キーデータとユーザから入力される暗号化／復号化用キーデータとの比較結果に基づいて前記可搬型記憶媒体に対するアクセス権の有無を判定し、アクセス権を有すると判定したとき、前記可搬型記憶媒体に対するデータ書き込み／読み出し要求に応じてライトデータの暗号化およびその暗号化データの書き込み／暗号化データの読み出しおよびその復号化を行うことを特徴とする。

【0009】このアクセス制御方法によれば、PCカードやフロッピーディスクなどの可搬型記憶媒体を暗号カードとして使用するための初期設定時には、可搬型記憶媒体の暗号化および復号化処理のためのキーデータ生成に用いるパスワードの入力がユーザに促される。そしてユーザから入力されたパスワードを可搬型記憶媒体に格納すると共に、そのデータを利用してキーデータを生成し、そのキーデータをユーザに提示する。このようにして、可搬型記憶媒体には、キーデータ生成に使用したパスワードだけが格納され、キーデータはアクセス制御方法を実現するためのI/O制御システムとして使用されるソフトウェア内部で保持管理される。

【0010】また、計算機システムに着脱自在に装着して使用されるという可搬型記憶媒体の特徴を考慮し、初期設定された可搬型記憶媒体が計算機システムに装着されたとき、あるいは装着された可搬型記憶媒体に対するデータ書き込み／読み出し要求が発行されたときに、アクセス権チェックが行われる。このアクセス権チェックでは、ユーザにパスワードではなく、キーデータを入力させ、それが、可搬型記憶媒体から読み出したパスワードから生成したキーデータと比較される。そして、アクセス権を有すると判定された場合には、データ書き込み／読み出し要求に応じてライトデータの暗号化およびそ

の暗号化データの書き込み／暗号化データの読み出しおよびその復号化を行う。

【0011】したがって、データ暗号化および復号化処理を介したデータI/O制御が行われ、記憶媒体単位でのデータの秘匿を実現することができる。さらにその秘匿においては、記憶媒体には実際にデータ暗号化および復号化の際に使用されるキーデータを格納しておくのではなく、あくまでもそのキーデータを生成するための元となるパスワードのみが格納されているので、第三者が記憶媒体内のデータを単純に解析しただけでは秘匿を解くことはできない。よって、個人単位で携帯され、且つ計算機システムに着脱自在に装着して使用されるという特徴を持つ可搬型記憶媒体のセキュリティー保持に適したアクセス制御を実現できる。

【0012】

【発明の実施の形態】以下、図面を参照してこの発明の実施形態を説明する。図1には、この発明の一実施形態に係るアクセス制御方法が適用される計算機システムとそのシステムで実行されるプログラムの機能構成が示されている。ここでは、計算機システムに取り外し自在に装着可能な可搬型記憶媒体として、半導体メモリを搭載したPCカードを例にとって説明する。

【0013】この計算機システムは、キーボードやマウスあるいはペンやトラックボールなどからなる入力装置1a、および表示装置1cを有する計算機本体を備えており、この計算機本体にはそれが電源オンの状態であってもPCカード1dの装着、取り外しを行うことができる。

【0014】処理制御装置1bは、入力装置1aより入力されたデータを判断することによりPCカード1dに対するI/Oリクエストを判別し、データ暗号化および復号化処理を介してPCカード1dへのデータI/O制御、また、これらの処理に応じて表示装置1cへの出力制御を行うものであり、その機能は計算機システム内のCPUによって実行されるソフトウェアであるPCカードドライバを利用して実現されている。

【0015】この処理制御装置1bは、入力装置1aより入力されたコード／位置データ1b1と表示装置1cに出力される文字データやグラフィックデータなどの出力データ1b2を処理する入出力処理部1b3と、計算機本体とPCカード1dとの着脱状態を検出する着脱検出処理部1b4と、入出力処理部1b3を介して処理された入力データよりPCカード1dに対するデータライトやデータリードなどのI/Oリクエストを判別するI/Oリクエスト判別処理部1b5と、I/Oリクエスト判別処理部1b5よりPCカード1dのフォーマットが要求された場合に、PCカード1dへのデータライトおよびデータリードにおけるデータ暗号化および復号化用キーデータの生成に使用するパスワードデータの入力とPCカード1dへの格納を行うパスワードデータ入力処

5

理部1 b 6と、パスワードデータ入力処理部1 b 6より入力・格納されたパスワードデータよりデータ暗号化／復号化用キーデータを生成する暗号化／復号化用キー生成処理部1 b 7と、PCカード1 dの装着時にデータ暗号化／復号化キーデータを使用してユーザのアクセス権をチェックするアクセスチェック処理部1 b 8と、PCカード1 dへのデータライト時に対象データを暗号化するデータ暗号化処理部1 b 9と、PCカード1 dへのデータリード時に対象データを復号化するデータ復号化処理部1 b 10と、PCカード1 dへのデータライトやデータリードなどのI/O処理を行うデータI/O処理部1 b 11と、データI/O処理部1 b 11にて使用するPCカードデータを管理するブロック管理情報データ1 b 12と、各処理部にて使用する変数やデータバッファとして利用するワークバッファ1 b 13より構成される。

【0016】また、PCカード1 dは、計算機本体からのデータI/Oコントロール処理信号に応じてコモンメモリ1 d 1やアトリビュートメモリ1 d 2へのデータリード／ライト制御を行うコントローラ1 d 3と、コントローラ1 d 3を介して計算機本体から送信されるデータを格納するコモンメモリ1 d 1と、PCカード1 dの属性情報が格納されているアトリビュートメモリ1 d 2により構成される。なお、これらのメモリは、フラッシュEEPROMなどの不揮発性メモリを使用して構成される。

【0017】図2は、ブロック管理情報データ1 b 12の構成図である。PCカードへ1 dのデータライトは、ハードディスク装置やフロッピディスク装置同様、ブロック（セクタ）単位でのデータI/O制御を行うため、PCカード内の総ブロック数データ2 aと、使用不能となった不要ブロックを管理するための不良ブロック数データ2 bと、不良ブロックとなったブロックNo. 1～Nデータ2 cと、不良になったブロックの代替先であるスペアブロックのスペアブロック数データ2 dと、スペアブロックの代替ブロック数であるスペアブロック登録数データ2 eと、スペアブロックNo. 1～Nデータ2 fを備えて構成する。

【0018】図3は、アトリビュートメモリ1 d 2の構成図である。アトリビュートメモリには、PCカードサイズ3 aと、スペアブロック数3 bと、製造メーカ名3 cと、リリースバージョン3 dと、パスワードデータ3 dなどのカード属性情報が格納されている。

【0019】以降、PCカードドライバを利用して実行されるPCカード1 dに対するアクセス制御の手順について説明する。まず、アクセス制御処理の基本的な流れについて説明する。

【0020】PCカード1 dのフォーマット時（暗号化カードとしての初期設定時）には、PCカード1 dに格納されるデータに対して暗号化処理を使用するかをユー

10

6

ザに選択させ、使用する場合に、その暗号化および復号化処理のための暗号化／復号化用キーデータを生成に用いるパスワードデータをユーザに入力させる。そして入力されたパスワードデータをPCカード1 d内に格納すると共に、そのデータを利用して暗号化／復号化用キーデータを生成し、そのキーデータをユーザにアナウンスする。

【0021】ユーザがPCカード1 dに対してライトリクエストした場合には、PCカード1 d内にパスワードデータが存在するかを確認し、格納されている場合にユーザに暗号化／復号化用キーデータを入力させ、PCカード1 dへのアクセス権をチェックする。その結果一致していたならば、キーデータを使用してデータを暗号化した後、PCカード1 d内にライトする。

【0022】また、ユーザがPCカード1 dに対してリードリクエストした場合には、PCカード1 d内にパスワードデータが存在するかを確認し、格納されている場合にユーザに暗号化／復号化用キーデータを入力させ、PCカード1 dへのアクセス権をチェックする。その結果一致していたならば、キーデータを使用してデータを復号化した後、リードリクエストコマンドにそのデータを送信する。

【0023】具体的には、以下のステップを利用してアクセス制御が行われる。

1) 計算機本体の入力装置1 aおよび表示装置1 cまたは音声出力機構を介して、ユーザへの入力や確認を促す入出力ステップ。

【0024】2) PCカード1 dと計算機本体との着脱状態を検出する着脱検出ステップ。3) PCカード1 dに対するI/O要求内容を取得しその内容を判断するI/Oリクエスト判別ステップ。

【0025】4) I/Oリクエスト判別ステップにより判別されたI/O内容がフォーマットである場合に、入出力ステップによりPCカード1 dに対してデータの暗号化を設定するか否かの選択を促し、選択結果を判断し暗号化設定が選択されたと判断した場合に、PCカード1 d内のデータを暗号化または復号化するために使用する暗号化／復号化キーの生成に使用するパスワードデータの入力を促し、入力されたパスワードデータを取得した後、PCカード1 d内に格納（記憶）するパスワードデータ入力ステップ。

【0026】5) PCカードフォーマット時にPCカード1 d内に格納されたパスワードデータを取得し、そのデータを元にデータ暗号化／復号化に使用されるキーデータを生成する暗号化／復号化用キー生成ステップ。

【0027】6) 暗号化／復号化用キー生成ステップにより生成された暗号化／復号化用キーデータをユーザにアナウンスするアナウンスステップ。

7) PCカード1 dに対するアクセス権を判断するためには、PCカード1 d内にパスワードデータが存在するか

40

50

7

否かを判別し、入出力ステップにより暗号化／復号化用キーデータ入力を促す表示を行い、これにより入力されたデータと、PCカード1 d 内に格納されたパスワードデータから生成したキーデータとを比較しアクセス権の合否を判定するアクセスチェックステップ。

【0028】8) 着脱検出ステップによりPCカード1 d が計算機本体に装着されたと判断され、アクセスチェックステップによりアクセス権を取得し、I/Oリクエスト判別ステップによりPCカード1 d に対してデータライトリクエストが判別された場合に、アクセスチェックステップにて生成されたキーデータを使用して対象となるライトデータを暗号化した後、PCカード1 d 内に格納するデータ暗号化ステップ。

【0029】9) 着脱検出ステップによりPCカード1 d が計算機本体に装着されたと判断され、アクセスチェックステップによりアクセス権を取得し、I/Oリクエスト判別ステップによりPCカード1 d に対してデータリードリクエストが判別された場合に、アクセスチェックステップにて生成されたキーデータを使用して対象となるPCカード1 d 内のデータであるリードデータを復号化した後、復号データをリクエスト側に渡すデータ復号化ステップ。

【0030】次に、図4のフローチャートを参照して、PCカード1 d へのアクセス制御処理の流れを具体的に説明する。このアクセス制御処理は、前述したように、計算機本体のメインメモリに常駐するPCカードドライバによって実現されており、計算機本体を起動した際にPCカード1 d の認識処理などが行われ、そのPCカード1 d に対するI/Oリクエスト待ちの状態になる。

【0031】計算機本体の入力装置1 a よりPCカード1 d に対するPCカードフォーマットやデータライトあるいはデータリードなどのI/Oリクエストコマンドが実行された場合、PCカードドライバは、コード／位置データ1 b 1 および入出力処理部1 b 3 を介して、I/Oリクエストを受け取る（ステップ4 a）。

【0032】そして、PCカード1 d が計算機本体に装着されているかを着脱検出処理部1 b 4 にて判別する（ステップ4 c）。その結果、PCカード1 d が装着されていない場合には、I/Oリクエストコマンドプログラムが保持しているステータスデータ内にエラーステータスをセットした後、I/Oコマンドプログラムに戻る（ステップ4 d、4 e）。

【0033】なお、本実施形態のPCカードドライバでは、計算機本体の起動開始から終了時までのPCカードの装着状態を計算機本体を介してPCカードが割り当てられたドライブごとに管理しており、それを着脱フラグとして保持している。

【0034】PCカード1 d が正常に装着されていた場合には、I/Oリクエスト判別処理部1 b 5 により受け取ったI/Oリクエストの内容を解析し、データI/O

10

8

処理部1 b 1 にてI/Oリクエストの内容に応じた処理を行う（ステップ4 f～4 i'）。

【0035】ここで、主なデータI/Oリクエストに対応する処理の流れについて説明する。

（PCカードフォーマット処理）I/Oリクエスト判別処理部1 b 5 により、受け取ったI/Oリクエストがフォーマットの場合、本PCカードドライバは、入出力処理部1 b 3 により計算機本体の表示装置1 c を介して、ユーザーに対して、データ暗号化および復号化処理機能付きのPCカードとしてフォーマットを行うかについての選択を促すために、選択用画面を表示する（ステップ4 f、4 g）。

【0036】その結果、ユーザーがデータ暗号化および復号化機能付きフォーマットを選択した場合には、パスワードデータ入力処理部1 b 6 より、データ暗号化／復号化用のキー（鍵）データの生成に使用するパスワードデータの入力をユーザーに促す画面を表示する（ステップ4 h、4 i）。

【0037】そして、入力されたパスワードを元に、暗号化／復号化用キー生成処理部1 b 7 によりデータ暗号化および復号化処理で使用する暗号化／復号化キーデータを生成し、表示装置1 c に表示してユーザーにアナウンスする（ステップ4 j）。そして、ユーザーが入力したパスワードデータをPCカード1 d 内のアトリビュートメモリ1 d 2 内にコントローラ1 d 3 を介して格納するとともに、ブロック管理情報データ1 b 1 2 など参照してPCカード1 d 内のメモリをフォーマットする（ステップ4 k）。そしてフォーマットコマンドプログラム内のステータスデータ内にステータス値をセットし、コマンドプログラムに処理を戻す（ステップ4 l）。

【0038】なお、データ暗号化および復号化付きフォーマットの確認ステップ（ステップ4 g）にて、ユーザーがデータ暗号化および復号化処理なしのフォーマットを選択した場合には、通常のフォーマット処理を行いステータス値をセットした後、コマンドプログラムに処理を戻す。

【0039】（データライト処理）I/Oリクエスト判別処理部1 b 5 により、受け取ったI/Oリクエストがデータライトの場合、本PCカードドライバは、PCカード1 d が挿入されているドライブに対応する脱着フラグの状態と、PCカード1 d 内のアトリビュートメモリ1 d 2 をチェックする（ステップ4 n）。その結果、データ暗号化用にフォーマットされたPCカード1 d が、アクセスチェック処理部1 b 8 を介してアクセス権を取得していない場合（例えば、アクセスチェックが一度も行われてない、またはアクセスチェック後にカードの着脱が行われている）は、アクセスチェック処理部1 b 8 により表示装置1 c を介して、画面上にデータ暗号化および復号化用キーデータの入力画面を表示し、ユーザーにデータ暗号化／復号化用キーデータの入力を促す（ステ

40

50

9

ップ4 o、4 p)。

【0040】そして、ユーザが入力したデータ暗号化／復号化用キーデータが有効かを判断するために、PCカード1 d 内のアトリビュートメモリ1 d 2内に格納されているパスワードデータよりデータ暗号化／復号化用キーデータを生成して比較を行う。比較の結果、キーデータが一致する場合は、そのキーデータを使用して、対象となるライトデータを暗号化処理部1 b 9により暗号化した後、コントローラ1 d 3およびアトリビュートメモリ1 d 2内データを介して、コモンメモリ1 d 1に格納する(ステップ4 t、4 v)。そして、ステータス値をセットした後、ライトコマンドに処理を戻す(ステップ4 w)。

【0041】なお、データ暗号化／復号化用キーデータの比較の結果、不一致の場合には、表示装置1 c の画面上にエラーメッセージを表示し、エラーステータス値をセットしてライトコマンドに処理を戻す(ステップ4 q～4 s)。

【0042】また、アクセスチェック処理部1 b 8にてアクセス権を取得してからPCカード1 d が脱着されていない場合には、アクセスチェックステップを行う必要がないと見なし、アクセスチェックなしで、データを暗号化する。また、PCカード1 d のアトリビュートメモリ内にパスワードデータが存在しない場合には、アクセスチェックおよびデータ暗号化ステップを行わずに、通常通りデータライトを行う。

【0043】(データリード処理) I/Oリクエスト判別処理部1 b 5により、受け取ったI/Oリクエストがデータリードの場合の処理は、上記データライト処理の流れとほぼ同様な処理が行われ、データ暗号化ステップの代わり、その部分でデータ復号化ステップが行われる。

【0044】すなわち、I/Oリクエスト判別処理部1 b 5により、受け取ったI/Oリクエストがデータリードの場合、本PCカードドライバは、PCカード1 d が挿入されているドライブに対応する脱着フラグの状態と、PCカード1 d 内のアトリビュートメモリ1 d 2をチェックする(ステップ4 y)。その結果、データ暗号化用にフォーマットされたPCカード1 d が、アクセスチェック処理部1 b 8を介してアクセス権を取得していない場合(例えば、アクセスチェックが一度も行われていない、またはアクセスチェック後にカードの着脱が行われている)は、アクセスチェック処理部1 b 8により表示装置1 c を介して、画面上にデータ暗号化および復号化用キーデータの入力画面を表示し、ユーザにデータ暗号化／復号化用キーデータの入力を促す(ステップ4 z、4 a')。

【0045】そして、ユーザが入力したデータ暗号化／復号化用キーデータが有効かを判断するために、PCカード1 d 内のアトリビュートメモリ1 d 2内に格納され

10

ているパスワードデータよりデータ暗号化／復号化用キーデータを生成して比較を行う。比較の結果、キーデータが一致する場合は、そのキーデータを使用して、対象となる暗号化データを読み出して復号化した後、それを要求元に渡す(ステップ4 e'、4 g')。そして、ステータス値をセットした後、ライトコマンドに処理を戻す(ステップ4 h')。

【0046】なお、データ暗号化／復号化用キーデータの比較の結果、不一致の場合には、表示装置1 c の画面上にエラーメッセージを表示し、エラーステータス値をセットしてリードコマンドに処理を戻す(ステップ4 b'～4 d')。また、アクセスチェック処理部1 b 8にてアクセス権を取得してからPCカード1 d が脱着されていない場合には、アクセスチェックステップを行う必要がないと見なし、アクセスチェックなしで、データを復号化する。また、PCカード1 d のアトリビュートメモリ内にパスワードデータが存在しない場合には、アクセスチェックおよびデータ復号化ステップを行わず

に、通常通りデータリードを行う。

【0047】以上の手順によれば、実際にデータの暗号化および復号化に使用するキーデータでなく、そのキーデータを生成するためにユーザに入力させたパスワードデータをPCカード1 d 内に格納することにより、キーデータはカード内部に物理的に存在しなくなり、第三者がPCカード内データを解析することによりパスワードデータを取得することができたとしても、データを復号することは困難となる。よって、データの秘匿を保持することができる。

【0048】また、計算機システムに着脱自在に装着して使用されるというPCカード1 d の特徴を考慮し、暗号化カードとして初期設定されたPCカード1 d に対するアクセスチェックが行われていない場合、またはアクセスチェック後にカードの着脱が行われている場合に、データ書き込み／読み出し要求に応答して、アクセス権チェックが行われる。このアクセス権チェックでは、ユーザにパスワードではなく、キーデータを入力させ、それが、可搬型記憶媒体から読み出したパスワードから生成したキーデータと比較される。そして、アクセス権を有すると判定された場合には、データ書き込み／読み出し要求に応じてライトデータの暗号化およびその暗号化データの書き込み／暗号化データの読み出しおよびその復号化を行う。したがって、PCカード1 d の着脱が行われても、アクセス権を正しく判定することができる。

【0049】このように、データ暗号化および復号化処理を介したデータI/O制御を行うことにより、個人単位で携帯され、且つ計算機システムに着脱自在に装着して使用されるという特徴を持つPCカード1 4などの可搬型記憶媒体のセキュリティー保持に適したアクセス制御を実現できる。

【0050】なお、図4では、データライト／リードの

50

11

度にアクセスチェックを行うか否かを判定したが、暗号化されたPCカード1dが新たに装着されたときに実行するカード認識処理にてアクセスチェックを行えば、その後、そのカード着脱が行われるまでは、アクセスチェックを省略しても良い。

【0051】この場合のカード認識処理およびI/O処理の手順をそれぞれ図5、図6に示す。PCカード1dが計算機本体に装着される度、PCカードドライバは、図5の手順でカード認識処理を行う。すなわち、その装着されたPCカード1dにパスワードが格納されているか否かに応じて、それが暗号化カードであるか否かを調べる(ステップS11)。暗号化カードでない場合には、それを通常の非暗号化カードとして認識する(ステップS14)。

【0052】パスワードが格納されている暗号化カードである場合には、PCカードドライバは、ユーザにデータ暗号化/復号化用キーデータの入力を促す。そして、ユーザが入力したデータ暗号化/復号化用キーデータが有効かを判断するために、PCカード1d内のアトリビュートメモリ1d2内に格納されているパスワードデータよりデータ暗号化/復号化用キーデータを生成して比較を行う(ステップS12)。比較の結果、一致していれば正当なそのカードが正当な暗号化カードであると認識され(ステップS13, S15)、不一致であれば、エラー発生の通知が行われる(ステップS16)。

【0053】このような認識処理が行われたカードを着脱することなく使用する場合においては、データライトリクエストおよびデータリクエストに応じて図6の処理が行われる。

【0054】すなわち、I/Oリクエスト判別処理部1b5により、受け取ったI/Oリクエストがデータライトの場合(ステップS21)、本PCカードドライバは、ライト対象のカードが暗号化カードとして認識されたものであるか否かを調べる(ステップS22)。暗号化カードとして認識されている場合には、フォーマット処理ですでに生成されているキーデータを利用して、ライトデータを暗号化した後にカードに書き込む(ステップS23, S24)。暗号化カードでない場合には、暗号化を行わずに、即座にデータ書き込みを行う(ステップS24)。

【0055】同様に、受け取ったI/Oリクエストがデータリードの場合は(ステップS25)、本PCカードドライバは、リード対象のカードが暗号化カードとして認識されたものであるか否かを調べる(ステップS26)。暗号化カードとして認識されている場合には、フォーマット処理ですでに生成されているキーデータを利用して、記憶データを復号化した後に読み出す(ステップS27, S28)。暗号化カードでない場合には、復号化を行わずに、即座にデータを読み出す(ステップS28)。

10

20

30

40

50

12

【0056】なお、この発明は上述した実施形態に限定されるものではなく、ユーザにデータ暗号化および復号化機能付きPCカードフォーマットの設定についての選択や、パスワードあるいは暗号化/復号化キーデータを入力を促す際のアナウンス手段として、音声出力装置による音声でのアナウンスを用いてもよい。また、データの暗号化および復号化処理として、本実施形態では具体的にその方式について述べなかったが、この方式については秘密鍵暗号方式や公開鍵暗号方式であっても良い。また、アクセス権をチェックする際に、キーデータが一致するまでのリトライ回数を複数回設けても良い。さらに、PCカード内に格納されるパスワードデータについて、本実施形態では、PCカード内のアトリビュートメモリ内に格納するように述べたが、コモンメモリ内であっても良い。

【0057】

【発明の効果】以上説明したように、本発明によれば、PCカードなどの可搬型記憶媒体単位でのデータの秘匿を実現することができる。さらにその秘匿においては、記憶媒体内には実際にデータ暗号化および復号化の際に使用されるキー(鍵)データを格納しておくのではなく、あくまでもそのキーデータを生成するための元となるパスワードデータのみを格納しておくことにより、第三者が記憶媒体を解析しただけでは秘匿を解くことができない。よって、個人単位で携帯され、且つ計算機システムに着脱自在に装着して使用されるという特徴を持つ可搬型記憶媒体のセキュリティー保持に適したアクセス制御を実現できる。

【面面の簡単な説明】

【図1】この発明の一実施形態に係るアクセス制御方法が適用される計算機システムの構成を示すブロック図。

【図2】同実施形態の計算機システムで使用されるPCカードのデータ管理構造を説明するための図。

【図3】同実施形態の計算機システムで使用されるPCカードのアトリビュートメモリのデータ構造を説明するための図。

【図4】同実施形態の計算機システムにおけるアクセス制御処理の流れを説明するフローチャート。

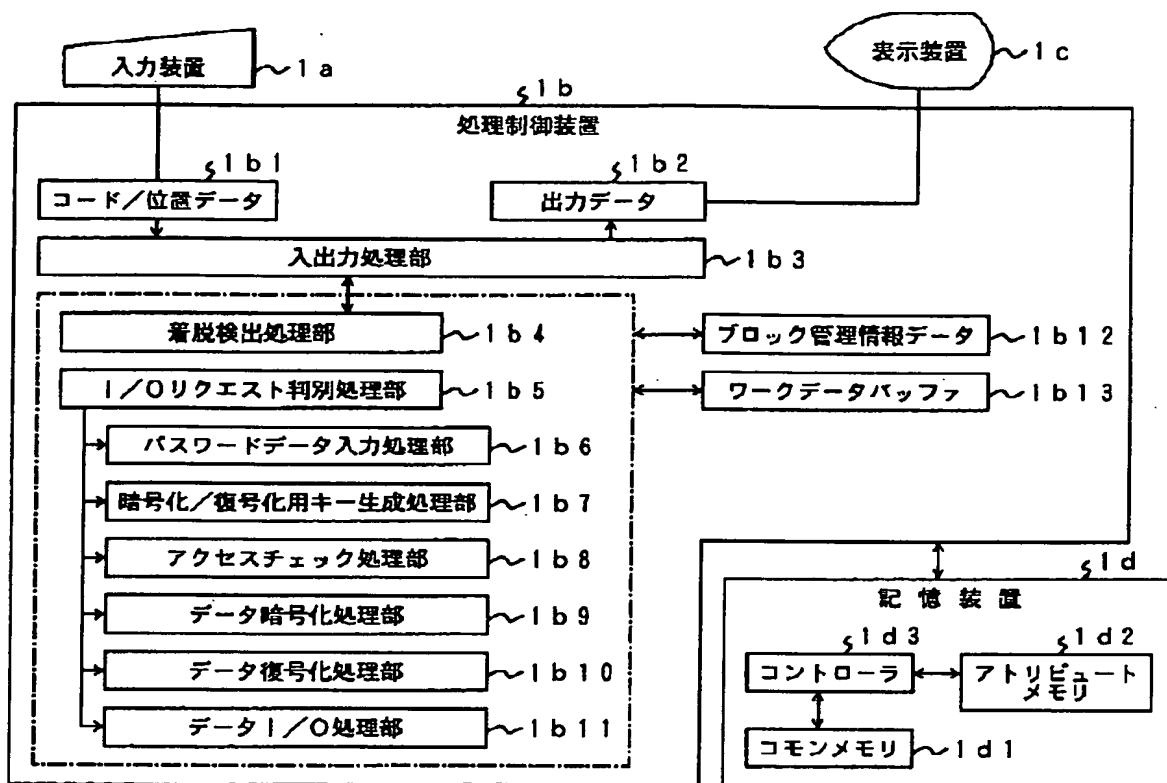
【図5】同実施形態の計算機システムにおけるカード認識処理の流れを説明するフローチャート。

【図6】図5のカード認識処理を行った場合におけるI/O処理の流れを説明するフローチャート。

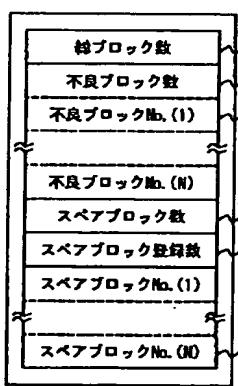
【符号の説明】

1b…処理制御装置、1d…PCカード、1b4…着脱検出処理部、1b5…I/Oリクエスト判別処理部、1b6…パスワードデータ入力部、1b7…暗号化/復号化用キー生成処理部、1b8…アクセスチェック処理部、1b9…データ暗号化処理部、1b10…データ復号化処理部、1b11…データI/O処理部。

【図1】

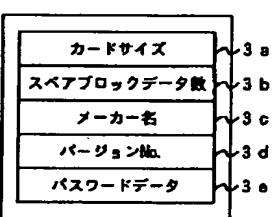


【図2】



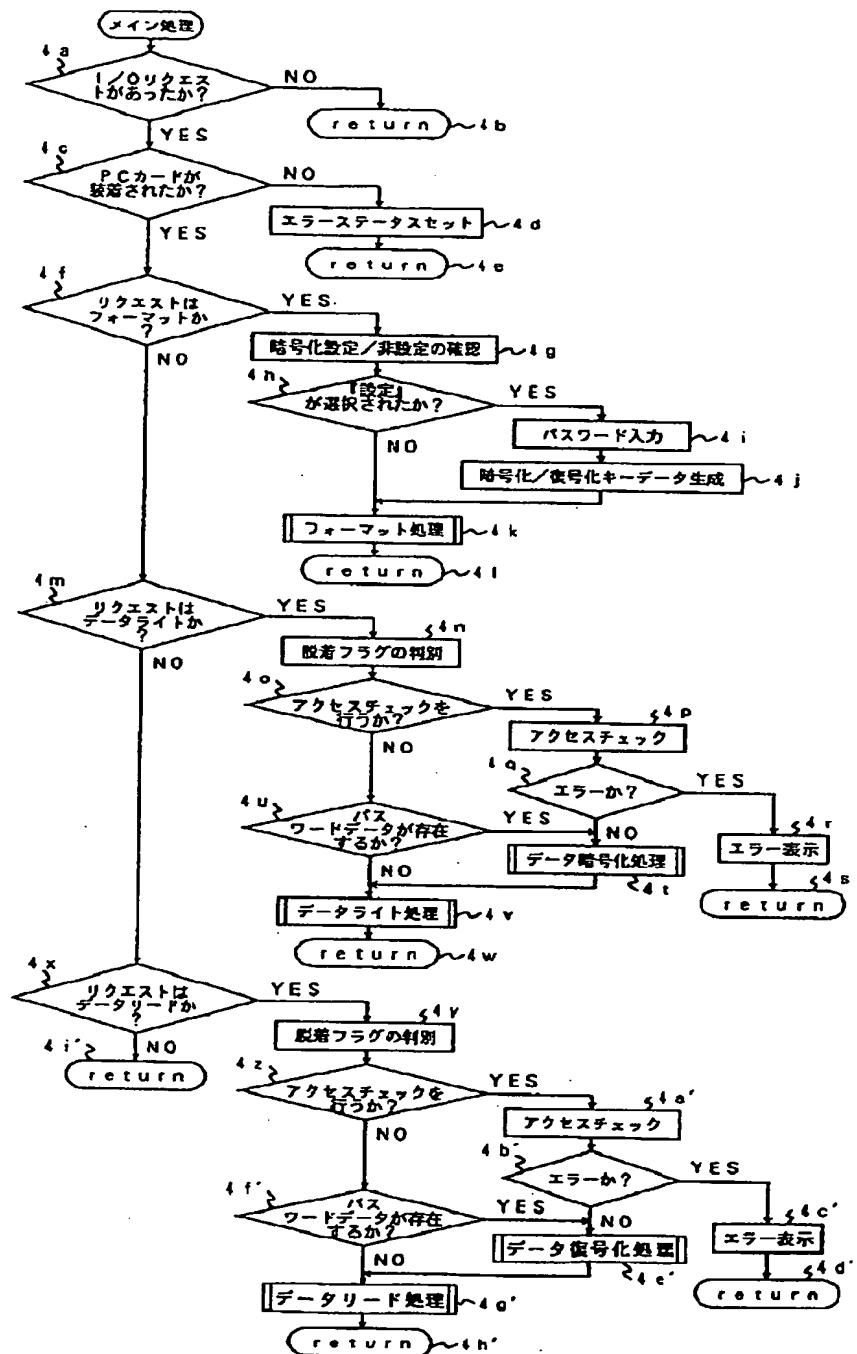
ブロック管理情報データ

【図3】

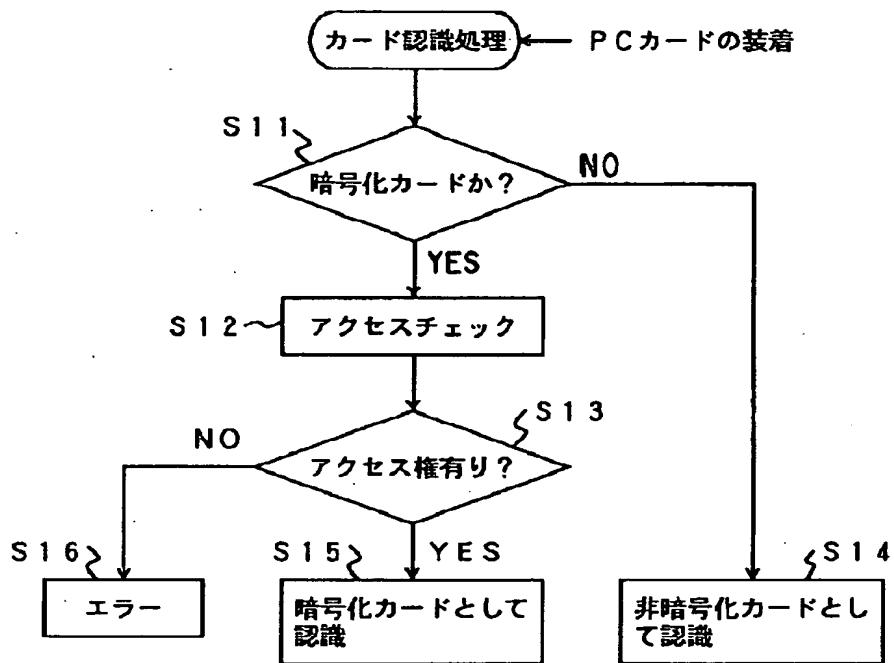


アトリビュートメモリ

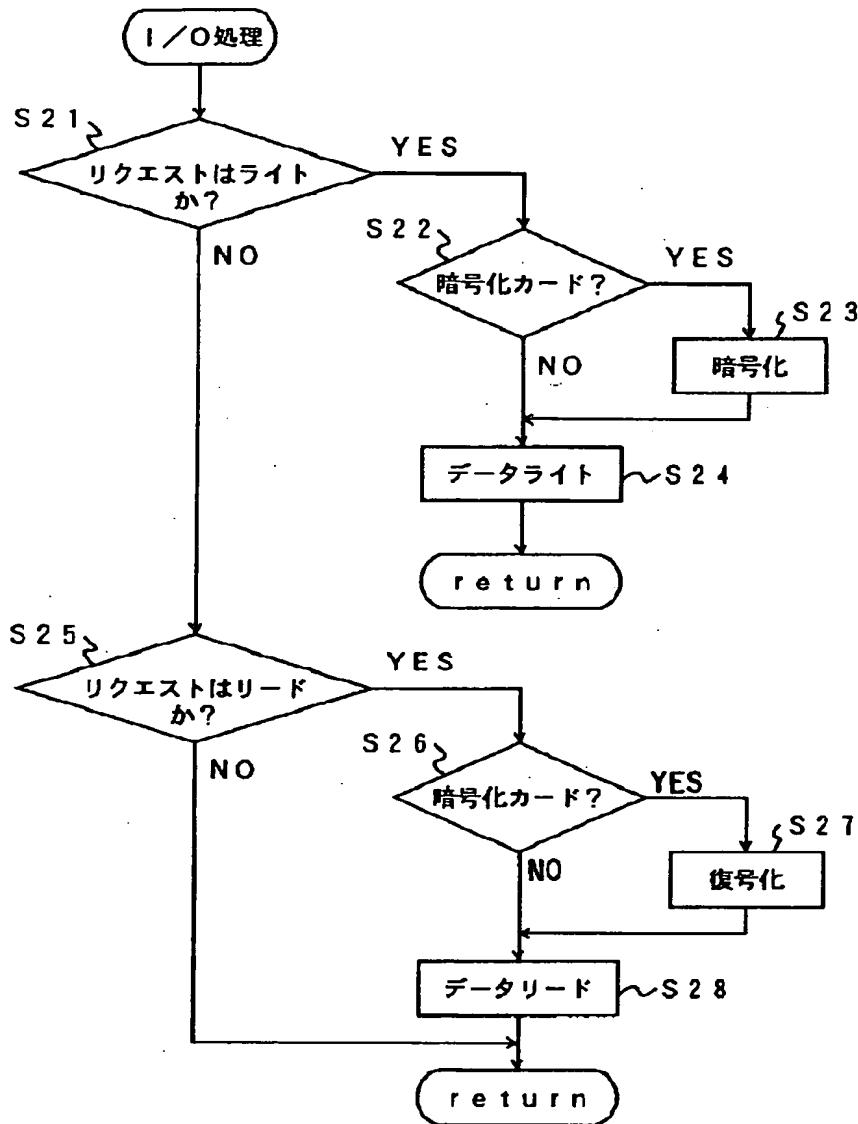
〔四〕



【図5】



【図6】



フロントページの続き

(51) Int.C1.⁶H04L 9/08
9/32

識別記号 庁内整理番号

F I
H04L 9/00

技術表示箇所

601Z
673A